CYBERSECURITY E SANITÀ: UN CAMBIO DI PARADIGMA

Ing. Lucia Scialacqua

DIPARTIMENTO DELL'AMMINISTRAZIONE GENERALE, DELLE RISORSE UMANE DEL BILANCIO
Ex Direzione generale della digitalizzazione, del sistema informativo sanitario e della statistica
MINISTERO DELLA SALUTE

La trasformazione digitale in Sanità

Cybersecurity in Sanità

… i temi legati alla cyber sicurezza devono accompagnare in modo **imprescindibile** questo percorso continuo verso la digitalizzazione…

> ***«La sanità è il settore più colpito a livello globale. In Italia gli attacchi alla sanità crescono dell'83%*** *rispetto al primo semestre 2023»*
>
> *Rapporto Clusit 2024- Edizione di metà anno, Ottobre 2024 : https://clusit.it/rapporto-clusit/*

Le **sfide** di cybersecurity del settore sanitario

- **Protezione dei dati sensibili**
- **Crescita degli attacchi ransomware**
- **Infrastrutture obsolete**
- **Dispositivi IoT e medici connessi**
- **Formazione insufficiente**
- **Interoperabilità e condivisione dei dati**
- **Attacchi alle infrastrutture critiche**
- **Regolamentazioni complesse**
- **Ottimizzazione delle risorse**
- **Minacce interne**

Soluzioni per affrontare le sfide

Protezione dei dati sensibili

Crittografia avanzata
Accesso controllato
Monitoraggio continuo

Crescita degli attacchi ransomware

Backup regolari
Segmentazione della rete
Simulazioni di attacco

Infrastrutture obsolete

Aggiornamenti regolari
Patch management
Virtualizzazione

Dispositivi IoT e medici connessi

Inventario e controllo
Micro segmentazione
Sicurezza pre-implementazione

Formazione insufficiente

Sensibilizzazione
Simulazioni regolari
Policy aziendali chiare

Interoperabilità e condivisione dei dati

Standard di sicurezza
Data masking
Accesso condizionato

Attacchi alle infrastrutture critiche

Piani continuità operativa
Protezione della rete
Supporto da enti sicurezza nazionale (ACN)

Regolamentazioni complesse

Compliance automation
Interpretazione normative
Audit regolari

Ottimizzazione delle risorse

Definizione priorità interventi
Approccio scalabile

Minacce interne

Controllo degli accessi
Monitoraggio degli utenti
Politiche disciplinari chiare

Quadro Normativo

Legge n. 90 del 28 giugno 2024 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

Punti rilevanti:
Inasprimento delle pene
Obbligo di notifica degli incidenti
Nomina di un referente per la cybersecurity
Rafforzamento del ruolo dell'ACN
Introduzione di nuove figure di reato

La **direttiva 2011/24/UE del Parlamento europeo e del Consiglio (NIS2)** rappresenta un **rafforzamento significativo** rispetto alla NIS1

Punti rilevanti:
1. Espansione dell'ambito di applicazione
2. Maggiore dettaglio sui requisiti di sicurezza
3. Miglioramento delle norme di notifica degli incidenti
4. Armonizzazione e coordinamento a livello UE
5. Definizione più puntuale delle competenze delle Autorità Nazionale e di Settore
6. Focus sulla catena di fornitura e la gestione delle terze parti
7. Maggior coinvolgimento della dirigenza

D.lgs. 138 del 2024: Recepimento della NIS2 in Italia, entrato in vigore il 16 ottobre 2024

D.lgs. 138 del 2024: Tavolo per l'attuazione della disciplina NIS

Agenzia per la Cybersicurezza Nazionale (ACN)

Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa:

a) La Presidenza del Consiglio dei ministri
b) il Ministero dell'economia e delle finanze
c) Il Ministero delle imprese e del made in Italy
d) il Ministero dell'agricoltura, della sovranità alimentare e delle foreste
e) il Ministero dell'ambiente e della sicurezza energetica
f) il Ministero delle infrastrutture e dei trasporti
g) il Ministero dell'università e della ricerca
h) il Ministero della cultura
i) **il Ministero della salute**

Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano: definizione delle modalità di collaborazione tra le Autorità di settore e le regioni e le province autonome di Trento e di Bolzano

Settore Salute: ambito di applicazione

Settori altamente critici

Settore	Tipologia di soggetto
Settore Sanitario	Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio
	Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio
	Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio
	Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2
	Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio

Settori critici

Settore	Sottosettore	Tipologia di soggetto
Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva

Settore Salute: Autorità NIS

Le **Autorità di settore NIS,** per i rispettivi settori e sotto settori di competenza, procedono:

- al supporto per verifica dei soggetti, individuazione dei soggetti essenziali e importanti e applicazione delle deroghe
- al supporto per le funzioni e per le attività di regolamentazione
- all'elaborazione dei contributi per la relazione annuale sull'attuazione del decreto
- all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione settoriale del presente decreto nonché al relativo monitoraggio
- alla partecipazione alle attività settoriali del Gruppo di Cooperazione NIS

Tavoli di Settore per contribuire all'efficace e coerente attuazione settoriale del decreto nonché al relativo monitoraggio

NIS Cooperation Group
Work Stream 12 - for cybersecurity in the health sector

Piano d'azione europeo per la cybersecurity negli ospedali e nei fornitori di servizi sanitari
Mapping of the policy and regulatory framework for health
Survey for "ENISA Foresight Cybersecurity Threats for 2030"

Iniziative di comunicazione pubbliche promosse da ACN

Iniziative di comunicazione pubblica promosse dall'Agenzia per la Cybersicurezza Nazionale (ACN) in occasione dell'entrata in vigore del decreto legislativo 4 settembre 2024, n. 138, che recepisce la Direttiva NIS2 (c.d. decreto NIS):

- una campagna di sensibilizzazione illustrata sul sito istituzionale di ACN (disponibile al seguente link: https://www.acn.gov.it/portale/w/l-acn-lancia-una-campagna-di-sensibilizzazione-sulla-nis2) realizzata attraverso la pubblicazione sul sito istituzionale di ACN di una sezione dedicata alla nuova disciplina NIS (https://www.acn.gov.it/portale/nis);

- la pubblicazione di un video introduttivo e della prima video-pillola sulla cybersecurity, realizzata in collaborazione con Marco Camisani Calzolari, mirati a promuovere una maggiore consapevolezza e una postura cyber.

Parola chiave:
MIGLIORAMENTO CONTINUO!

Monitoraggio della strategia di Cybersecurity Governance - Il miglioramento continuo
https://www.acn.gov.it/portale/

Grazie
per la Vostra cortese attenzione